Amendments to the Specification:

Please replace the paragraph beginning at page 1, line 12, with the following redlined paragraph:

The coverage area of WLAN is called ~~as~~ a service area, which is usually divided into Basic Service Area (hereinafter referred as BSA) and Extended Service Area (hereinafter referred as ESA); wherein BSA refers to the communication coverage area determined by transceivers of individual units in the WLAN and the geographic environment and is usually called ~~as~~ a cell, the scope of which is generally small; the method shown in Figure 1 is usually used to extend the coverage area of WLAN, *i.e.*, the BSA is connected to the backbone network (usually a wired LAN) via the APs and the wireless gateway, so that mobile hosts (MHs) in the BSA are connected to the backbone network via the APs and the wireless gateway to constitute a ESA.

Please replace the paragraph beginning at page 1, line 22, with the following redlined paragraph:

Compared with wire transmission, the confidentiality of wireless transmission is lower; therefore, to ensure communication security between the APs of the cell and the mobile hosts, information should be encrypted with keys before transmitted. When a mobile host moves across cells or powers on, it searches for the local cell, registers itself to the AP of the cell, and obtains information related with the cell; therefore, the encryption communication between the mobile host and the APs will be restricted to some extent. In detail, for example, when the mobile host MH12 moves from cell 1 into cell 2, if AP11 and ~~AP12~~ AP21 ~~is~~ are in the coverage area of the same key management server, then the encryption communication between mobile host MH12 and AP11 can be smoothly transited to between MH12 and AP21; however, if AP11 and AP21 are managed by different key management servers, then encryption communication between MH12 and AP21 can not be realized directly in cell 2 because AP21 can not obtain the communication key of MH12. However, if the mobile host MH12 sends its key to AP21 through the wireless channel without encryption, the system will be vulnerable because the key may be intercepted and deciphered easily.

Please replace the paragraph beginning at page 3, line 9, with the following redlined paragraph:

As shown above, the method of the present invention combines a key distribution process with an authentication process of the mobile hosts and utilizes an authentication device to manage key distribution, so that mobile hosts can roam in a scope larger than the coverage area of the key management server. Because the key distribution does not involve transmitting the key which is not encrypted via the air interface, the method ensures the key is safe. In addition, said method does not depend on specific authentication modes, so it can be used under different kinds of WLAN protocols. Finally, because the AP does not need to manage user information, the method simplifies the AP structure, and thus lowers the cost.

Please replace the paragraph beginning at page 5, line 10, with the following redlined paragraph:

The mobile host MH12 establishes a connection with AP21 and sends an authentication request containing identity information to the authentication server in the backbone network 4 for authentication via AP21 and the wireless gateway 51. When receiving the authentication request, the authentication server authenticates the mobile host according to the identity information I contained in the authentication request; if the identity information I is inconsistent with the stored one, the authentication server deems the mobile host as an illegal one and rejects the authentication request, and then sends an ACCEPT_REJECT message to ~~MH11~~ MH12 via the wireless gateway 51 and AP21; if the identity information I contained in the authentication request is consistent with the stored one, the authentication server deems the mobile host as a legal one and accepts the authentication request, and then, as shown in Figure 2a, the authentication server searches for the corresponding property information P of the mobile host MH12 according to the identity information I and then sends it to AP21 via the wireless gateway 51. When receiving the property information P sent from the authentication server, AP21 sends a confirmation message back to the authentication server via the wireless gateway for safe receipt of the property information P and generates a key from the property information P with the key generation algorithm. The key generation algorithm can be any kind of algorithm, and the length of the key is free. When receiving the confirmation message from AP21, the authentication server sends an ACCESS_ACCEPT message to ~~MH21~~ MH12 via the wireless gateway 51 and AP21.

When receiving the ACCESS_ACCEPT message, the mobile host ~~MH21~~ MH12 generates a key from the property information P stored in itself with the same key generation algorithm as the one with which AP21 generates a key, and then encrypts data packets to be sent to AP21 with the key, and sends the encrypted data packets to AP21; ~~MH21~~ MH12 adds an encryption identifier in the data packets when encrypting the data packets. When receiving the data packets from ~~MH21~~MH12, AP21 detects the encryption identifier in the data packets; if the encryption identifier is found, AP21 decrypts the data packets with the key obtained from property information P and the key generation algorithm, and then forwards the decrypted data packets to the external network 4 via the wireless gateway 51; otherwise AP21 directly forwards the original data packets to the external network 4 via the wireless gateway 51.

Please replace the paragraph beginning at page 6, line 13, with the following redlined paragraph:

Figure 2b is a schematic diagram of the encryption communication method in WLAN according to another embodiment of the present invention. The difference between this embodiment and that of Figure 2a is: in the communication process, the key is generated with any key generation algorithm and then encrypted with property information P by AP21, and then sent to ~~MH21~~MH12. When receiving the key from AP21, ~~MH21~~ MH12 decrypts the key with the property information P stored in itself, encrypts the data packets to be sent to AP with the decrypted key and sends them to AP. ~~MH21~~ MH12 also adds an encryption identifier in the data packets when encrypting the data packets. In this case, each of the mobile hosts does not need to know the key generation algorithm used by AP21.

Please replace the paragraph beginning at page 7, line 1, with the following redlined paragraph:

Figure 2d is a schematic diagram of the encryption communication method in WLAN according to another embodiment of the present invention. The difference between this embodiment and that of Figure 2c is: when the authentication succeeds, the authentication server generates the key with the key generation algorithm and then sends the key to AP21, and at the same time, the authentication server also sends the key encrypted with the property information P to ~~MH21~~MH12.

Please replace the paragraph beginning at page 7, line 12, with the following redlined paragraph:

In above embodiments, if the mobile hosts are authenticated by the wireless gateway 51 to 53 independently, other functions of authentication server can also be implemented on the wireless gateways, for example, wireless gateways 51 to 53 can be configured to send ACCESS_ACCEPT message to ~~MH21~~MH12, generate the key, and send property information P to AP21, etc. Similarly, if the confirmation function is implemented by the authentication server and the wireless gateways interoperably, other functions of the authentication server can also be implemented by the authentication server and the wireless gateways interoperably. In general, all functions of the authentication server can be implemented by the authentication device.